

#4  
ZMP

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
in this Office.

出 願 年 月 日  
Date of Application:

1999年 9月24日

願 番 号  
Application Number:

平成11年特許願第271022号

願 人  
Applicant(s):

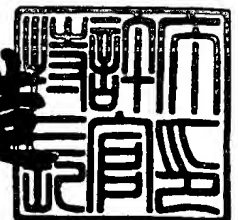
溝部 達司  
澤口 高司

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 8月 4日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



【書類名】 特許願

【整理番号】 SM199909

【提出日】 平成11年 9月24日

【あて先】 特許庁長官 殿

【国際特許分類】 G06K 9/00  
G06F 15/62

【発明者】

    【住所又は居所】 東京都新宿区高田馬場 3 - 4 0 - 1 3

    【氏名】 澤口 高司

【特許出願人】

    【識別番号】 000168207

    【氏名又は名称】 溝部 達司

【特許出願人】

    【識別番号】 596132905

    【氏名又は名称】 澤口 高司

【代理人】

    【識別番号】 100064414

    【弁理士】

    【氏名又は名称】 磯野 道造

【手数料の表示】

    【予納台帳番号】 015392

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9722612

    【包括委任状番号】 9607741

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 携帯個人認証装置及び同装置によりアクセスが許可される電子システム

【特許請求の範囲】

【請求項 1】 携帯可能に構成され、通信手段を内蔵すると共に、人間の生物学的特徴のうち少なくとも一つを読み取る読取手段を有し、この読み取ったデータを認証データとして、この認証データに基づいて個人の認証を行うこと、を特徴とする携帯個人認証装置。

【請求項 2】 前記認証が、人間の指紋、声紋、網膜紋、虹彩紋、顔、署名、のうち少なくとも一つを利用したバイオメトリクス認証であり、

前記読取手段はこのバイオメトリクス認証に対応して、人間の指紋、声紋、網膜紋、虹彩紋、顔、署名、のうち少なくとも一つを読み取ることができるものであること、

を特徴とする請求項 1 に記載の携帯個人認証装置。

【請求項 3】 前記携帯個人認証装置は、個人認証を前提として利用者のアクセスが可能となる電子システムにおける個人認証に使用され、

前記読み取った認証データにより、前記電子システムの利用を意図する利用者がこの電子システムへのアクセスの許可を受けること、を特徴とする請求項 1 又は請求項 2 に記載の携帯個人認証装置。

【請求項 4】 前記電子システムが通信ネットワーク上を流通する電子情報に貨幣的価値を与えて電子貨幣を設定し、この電子貨幣により商取引の決済を行う電子商取引システムであり、

前記携帯個人認証装置は、この電子商取引システムが要求する個人認証のための認証データの入力を行うと共に、

所定の金融機関の口座から所定の金額の預貯金を引き出し、これを電子貨幣として記憶部に格納し、この格納した電子貨幣により前記商取引の決済を行うこと、ならびに前記決済後の電子貨幣の残高及びその使用履歴を前記格納部に残すこと、

を特徴とする請求項 1 乃至請求項 3 のいずれか 1 項に記載の携帯個人認証装置。

【請求項 5】 前記電子システムがクレジット情報により決済を行う電子商取引システムであり、

前記携帯個人認証装置は、この電子商取引システムが要求する個人認証のための認証データの入力を行うと共に、

クレジット情報が格納される格納手段を有すること、  
を特徴とする請求項 1 乃至請求項 3 のいずれか 1 項に記載の携帯個人認証装置。

【請求項 6】 前記電子商取引システムが通行料金を自動的に徴収する自動料金収受システムであることを特徴とする請求項 4 又は請求項 5 に記載の携帯個人認証装置。

【請求項 7】 前記電子システムが緊急事態発生時に所轄のセンタに緊急連絡を行う通報システムであり、

前記携帯個人認証装置は、少なくとも前記緊急連絡を解除する際の解除連絡に使用され、

前記解除連絡を行う際には、この携帯個人認証装置により読み取った認証データを前記通信手段により前記所轄のセンタに送信すること、  
を特徴とする請求項 3 に記載の携帯個人認証装置。

【請求項 8】 前記生物学的特徴の一つを指紋とし、前記携帯個人認証装置は P C カードスロットを有し、この P C カードスロットに前記指紋を読み取る読取手段を備えた P C カードを挿入することで本人の認証を行うことを特徴とする請求項 1 乃至請求項 7 のいずれか 1 項に記載の携帯個人認証装置。

【請求項 9】 請求項 3 乃至請求項 8 のいずれか 1 項に記載の携帯個人認証装置によりアクセスが許可される電子システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、もっぱら個人の認証を行ったり個人認証を前提とする電子システムなどに使用される携帯個人認証装置及び同装置によりアクセスが許可される電子システムに関し、例えば、セキュリティ管理、電子商取引、あるいは、自動車事故、海山における遭難事故等における緊急連絡に用いて好適な、携帯個人認証装

置及び同装置によりアクセスが許可される電子システムに関する。

【0002】

【従来の技術】

従来から現金の代用として、所定の電子データを個人情報とともにＩＣカード、クレジットカード、デビットカード、スーパーカード等に記憶させ、その電子データの交換によって支払いを行う電子決済システムが知られている。

一方、最近では、インターネット等通信ネットワークを用いた電子商取引が実現しつつある。これに伴い、電子商取引に関する決済をネットワーク上で行う技術が各種提案されている。代表的には、クレジットカード決済であり、あるいは、実際の紙幣と同じ価値を持つ電子マネーを用いたキャッシュ決済である。

【0003】

このような状況の中、誰もがインターネットに接続されているコンピュータにアクセスする可能性が生まれ、正当な利用者か、正当な情報かを判断する電子認証の重要性が高まってきている。加えて企業がインターネットを商取引等重要な業務に利用し始めたため、ネットワーク社会での電子的な身分証明は必須となっている。

【0004】

また、最近、自動車のエアバックの作動を契機として、その事故情報を消防署や警察、保険会社等所轄のセンタに緊急連絡する通報システムが実現されようとしている。ところが、エアバックが作動しても事故が軽微なこともあり、機器の誤動作もある。事故が軽微な場合、本人がその緊急連絡システムを解除すれば問題ないが、大事故の場合に、誰かが故意に、あるいは誤って解除することが有り得る。この場合、連絡した人間が本人であるか否か等の認証が重要になる。

【0005】

【発明が解決しようとする課題】

上述した電子商取引において、ＩＣカード等の記憶媒体を用いて電子決済を行う場合、あるいはクレジットカードによる決済を行う場合は、第三者による不正使用を防御するため、利用の都度パスワード入力による利用者の認証が必要となり、操作や処理が煩雑となる欠点があり、また、防御をかけない場合は、そのＩ

Cカード等に設定された金額の全てが第三者による不正使用の危険にさらされるといった欠点を有している。

【0 0 0 6】

また、インターネットを用いて電子商取引を行う場合、前者は、クレジットカードを必要とし、カード番号等セキュリティを必要とする情報をなんらかの方法により送信する必要がある、ICカードを利用して電子決済を行うのと同じ欠点を持つ。

更に、上述した自動車事故等の通報システムにおいても同様、緊急連絡解除の際に信用性の高い本人認証のための手段が要求され、通報あるいは通報解除の確度が高いものが期待される。

上記に限らず、どこでも簡便に個人の認証を行うことのできる手段が、今後必要になると考える。また、カード社会においてはカードが氾濫し、何枚ものカードを携帯しなければをらない煩わしさや、カードを管理しなければならない煩わしさがある。

そこで、本発明は、上記課題を解決し、今後の社会において必要不可欠となる個人の認証をどこでも行え、あらゆる用途に使用することのできる携帯個人認証装置及び同装置によりアクセスが許可される電子システムを提供することを目的とする。

【0 0 0 7】

【課題を解決するための手段】

上述した課題を解決した請求項 1 に記載の携帯個人認証装置は、携帯可能に構成され、通信手段を内蔵すると共に、人間の生物学的特徴のうち少なくとも一つを読み取る読取手段を有し、この読み取ったデータを認証データとして、この認証データに基づいて個人の認証を行うことを特徴とする。

この携帯個人認証装置は、今後一人一台程度所持するであろう携帯電話やPDAなどの携帯機器をベースとして構成したり、携帯電話やPDAの機能を併せ持たせるのが好適である。個人の認証を行うに際しては、入力された認証データ（読み取ったデータ）とあらかじめ登録してある参照データとを対比することになるが、あらかじめ登録してある参照データは、携帯個人認証装置内に格納される

こととしても良い。また、あらかじめ登録してある認証データは、携帯個人認証装置以外の例えばサーバ（発明の実施の形態でいう「認証サーバ」）などに格納されることとしても良い。この場合は、例えば、入力された認証データを通信手段によりサーバ側に送信し、サーバ側で行った認証結果を通信手段により得る。この携帯個人認証装置は、例えば、警察における不審者尋問や警備会社などにおける警備に用いることができる。また、これに限らず広く個人の認証に用いることができる。

なお、通信手段は、有線・無線を問わない。

#### 【0008】

また、請求項2に記載の携帯個人認証装置は、前記認証が、人間の指紋、声紋、網膜紋、虹彩紋、顔、署名、のうち少なくとも一つを利用したバイオメトリクス認証であり、前記読取手段はこのバイオメトリクス認証に対応して、人間の指紋、声紋、網膜紋、虹彩紋、顔、署名、のうち少なくとも一つを読み取ることができるものであることを特徴とする。

これらは、個人に特有のものであり、パスワードのごとく個人が記憶しておく必要がない。また、カギなどの物品のごとく置き忘れるということもない。読取手段としては、声紋に対してはマイクロフォンが、指紋、網膜紋、虹彩紋、顔、署名に対してはCCDカメラが、指紋、署名に対してはスキャナがあげられる。

#### 【0009】

また、請求項3に記載の携帯個人認証装置は、個人認証を前提として利用者のアクセスが可能となる電子システムにおける個人認証に使用され、前記読み取った認証データにより、前記電子システムの利用を意図する利用者がこの電子システムへのアクセスの許可を受けることを特徴とする。

前記のとおり個人の認証を行うに際しては、入力された認証データ（読み取ったデータ）とあらかじめ登録してある参照データとを対比することになるが、あらかじめ登録してある参照データは、携帯個人認証装置内に格納されることとしても良い。この場合は、認証結果を電子システムに送信する。あるいは、認証結果を携帯認証装置に表示する。また、あらかじめ登録してある認証データは、電子システムが有するサーバなどに格納されることとしても良い。この場合は、例

えば、入力された認証データを電子システム側に送信する。

なお、特許請求の範囲における用語「アクセス」には、発明の実施の形態のように、SOS信号を解除するために通信を行い、該SOS信号を解除する行為なども含まれる。また、特許請求の範囲における用語「電子システム」は、電子商取引システム、道路や駐車場などの自動料金収受装置、自動販売機、公衆電話回線（ISDNを含む）、パソコン、LAN（有線・無線）、インターネットなどがあげられる。ちなみに、自動販売機の場合には、例えば有線（又は無線）で携帯個人認証装置と自動販売機を接続し、携帯個人認証装置側で認証データを入力し（読み取り）、この入力された認証データを自動販売機に送信して、取引可能とする構成とすることができる。また、LANの場合は、端末のパソコンに携帯個人認証装置を有線（又は無線）で接続し、携帯個人端末装置側で認証データを入力し、この入力された認証データをパソコン側に送信し、パソコンあるいはサーバで判断して、パソコンの使用及び／又はサーバへのアクセスを可能とする構成とすることができる。

#### 【0010】

また、請求項4に記載の携帯個人認証装置においては、前記電子システムが通信ネットワーク上を流通する電子情報に貨幣的価値を与えて電子貨幣を設定し、この電子貨幣により商取引の決済を行う電子商取引システムであり、前記携帯個人認証装置は、この電子商取引システムが要求する個人認証のための認証データの入力を行うと共に、所定の金融機関の口座から所定の金額の預貯金を引き出し、これを電子貨幣として記憶部に格納し、この格納した電子貨幣により前記商取引の決済を行うこと、ならびに前記決済後の電子貨幣の残高及びその使用履歴を前記格納部に残すこと、を特徴とする。

なお、この携帯個人認証装置を携帯通信端末装置として持つ電子商取引システムは、通信ネットワーク上を流通する電子情報に貨幣的価値を与えて電子貨幣を設定し、この電子貨幣により商取引の決済を行う電子システムであり、個人の認証を前提としている。

この電子貨幣の種類としては、ICカード型、ネットワーク型のどちらも含むものであり、特に限定しない。また、この電子貨幣の種類としては、クローズド



型、オープン型のどちらも含むものであり、特に限定しない。なお、オープン型の電子貨幣は、使用された後、すぐに決済されて現金化されずに、他人に移転することができる電子貨幣である。

【 0 0 1 1 】

また、請求項 5 に記載の携帯個人認証装置においては、前記電子システムがクレジット情報により決済を行う電子商取引システムであり、前記携帯個人認証装置は、この電子商取引システムが要求する個人認証のための認証データの入力を行うと共に、クレジット情報が格納される格納手段を有することを特徴とする。

なお、この携帯個人認証装置を携帯通信端末装置として持つ電子商取引システムは、前記商取引の決済をクレジット方式で行う電子システムであり、個人の認証を前提としている。

【 0 0 1 2 】

また、請求項 6 に記載の携帯個人認証装置においては、前記電子商取引システムが通行料金を自動的に徴収する自動料金収受システムであることを特徴とする。

通行料金を自動収受する自動料金収受システムとしては、E T C (Electric Toll Collection) が知られる。携帯個人認証装置により、自動車に搭載される E T C の車載装置の作動を可能とする（自動料金収受の認証を行う）。

あるいは、E T C の路上装置と携帯個人認証装置とで直接通信を行う構成とすることもできる。この場合、E T C の車載装置が不用になる。

【 0 0 1 3 】

また、請求項 7 に記載の携帯個人認証装置においては、前記電子システムが緊急事態発生時に所轄のセンタに緊急連絡を行う通報システムであり、前記携帯個人認証装置は、少なくとも前記緊急連絡を解除する際の解除連絡に使用され、前記解除連絡を行う際には、この携帯個人認証装置により読み取った認証データを前記通信手段により前記所轄のセンタに送信することを特徴とする。

なお、この携帯個人認証装置を携帯通信端末装置として持つ電子システムたる通報システムは、例えば、車両などに全地球測位システムの衛星電波を受信する機器を搭載し、緊急事態発生時に管轄センタに緊急連絡を行う。この通報システ

ムは、緊急事態発生時、前記搭載機器により、少なくとも前記衛星電波により測位された現在位置データを携帯通信回線ネットワーク経由で発信して緊急連絡を通報する。この通報システムにおける緊急連絡の通報の解除は、携帯個人認証装置により前記所轄のセンタに連絡をとる。この際、携帯個人認証装置で読み取った認証データを、通信手段によりセンタに送信し、センタのサーバなどにあらかじめ登録済みの参照データと照合し、その照合結果に基づき、前記緊急連絡の解除を有効とする。

さらに、海や陸での事故並びに遭難の際に、携帯個人認証装置により、認証データを送信すると共に、緊急連絡を行う構成としても良い。緊急連絡の解除の際と同様、個人の特定・悪戯などの防止に有効である。

【0014】

また、請求項8に記載の携帯個人認証装置は、前記生物学的特徴の一つを指紋とし、前記携帯個人認証装置はPCカードスロットを有し、このPCカードスロットに前記指紋を読み取る読取手段を備えたPCカードを挿入することで本人の認証を行うことを特徴とする。

【0015】

そして、請求項9に記載の発明は、携帯個人認証装置によりアクセスが許可される電子システムである。

【0016】

上述したように、本発明は、広く個人の認証を行うものである。また、通信ネットワーク上を流通する電子情報に貨幣的価値を与えて電子貨幣を設定し、この電子貨幣により商取引の決済を行う電子商取引の本人認証を行うための手段として、また、契約、決済のための手段として携帯通信端末装置を使用する。この携帯通信端末装置は、内蔵する通信手段を介して所定の金融機関の口座から任意の金額の預貯金を引き出し、また、これを電子貨幣として格納する格納手段を有し、この格納した電子貨幣により前記商取引の決済を行ない、決済後の電子貨幣の残高及びその使用履歴を記録する。

【0017】

このように、携帯通信端末装置（携帯個人認証装置が兼ねる）に、従来ICカ

ード等が持っていた電子財布的な機能を内包させることにより操作上の煩わしさから解放すると共に、生物学的特徴である、指紋、声紋、虹彩紋、網膜紋、顔、署名のバイオメトリクスのうち少なくとも1つを本人認証のための手段として使用することにより、セキュリティ機能の充実がはかれる。

また、A T M機器（一例としてのA T M機器）と接続することによって電子財布としての一元管理を実現する。更に、そのモバイル機器を使用して、銀行、証券会社、保険会社、信販会社、百貨店、スーパー、運輸等々、流通系の各企業が構築するサービスシステムを、例えば、インターネットやA T Mオンラインを利用して取り込み、交信することによって、発受注に関する契約、あるいは決済、契約解除等の指示を容易に行うことができる。

#### 【 0 0 1 8 】

更に、交通事故、遭難事故等発生の際、所轄センタへの緊急連絡解除時の本人認証のための手段としても本発明の携帯通信端末装置を用いることができる。この場合、全地球測位システム（G P S）の衛星電波を受信できる機器を介して現在位置等を知らせるS O S信号を携帯通信回線経由で所轄のセンタに通報するが、緊急連絡解除の際に本人認証を行い、機器の誤作動による、あるいは悪意の緊急連絡解除を防止することができ、このことにより、通報の確度が向上する。

#### 【 0 0 1 9 】

##### 【発明の実施の形態】

以下、発明の実施の形態を、図面を参照して詳細に説明する。

図 1 は、本発明の携帯個人認証装置が携帯通信端末装置として使用される電子商取引の一実施形態を示すブロック図である。図において、1 は銀行営業店システムであり、窓口にA T M機器 1 1 を有する。2 は、証券会社、保険会社、信販会社、百貨店、スーパー、運輸等の流通系システムであり、この中に銀行が含まれることもある。流通系システム 2 は、流通系ホスト 2 1 を核とし、遠隔地にP O S端末 2 1 が分散配置されている。

#### 【 0 0 2 0 】

3 は銀行計算機センタであり、銀行ホスト 3 1 を核に各銀行営業店システム 1 とは専用回線 4 を介して接続されている。また、エンドユーザは、本人認証のた

めにあらかじめ指紋が採取され、その情報は認証サーバ32に格納されてあるものとする。利用の都度、この認証サーバ32による本人照合が行われ、セキュリティの保護がなされる。

#### 【0021】

以下に示す実施形態では本人照合のための手段として、犯罪捜査等において実績のある指紋を使用するものとするが、他に個人の識別を確実にできるものとして声紋、虹彩紋、網膜紋があり、そのいずれを用いても構わない。参考のために、指紋、声紋、虹彩紋について定義すると、指紋とは、指頭の掌側面に見られる皮膚隆線のなす紋理をいい、その形状から弓状紋、蹄状紋、渦状紋に大別される。各紋型の出現頻度には、指種、左右、性別、人種等により差異がある。指紋は、胎生3~4カ月で形成され、その形態は、全く同じものは2つとなく、また、一生不変であることから個人の識別に利用される。

声紋とは、人間の声を周波数分析した結果をソナグラフで表したものをいう。また、虹彩紋とは、眼球の水晶体の前面にあって瞳孔を囲む輪状の膜である虹彩（アイリス）の模様をいう。虹彩は、脈絡膜が伸びて出来たもので、放射状に瞳孔開大筋、輪状に瞳孔活躍筋が並ぶ。光に対して反射的に働き、瞳孔の開閉や明暗調節を行う。含まれる色素によって茶眼、青眼等になる。

尚、認証は、上述した人間の生物学的特徴にとらわれず、顔写真、署名等の筆跡を用いても構わない。

#### 【0022】

説明を図1に戻す。5はエンドユーザであり、エンドユーザ5が持つ携帯通信端末装置51、例えば、携帯電話、PDA（Personal Data Assistants）等のモバイル機器は、銀行営業システム1が持つATM機器11、ならびに流通系システム2が持つホスト21とは、公衆回線網6経由で接続される。また、公衆回線網6に接続されないシステムとして自動販売機システム7があり、携帯通信端末装置51とは、後述するようにオフラインで接続される。

尚、上述した銀行、流通系のシステム1、2は、電子通貨発行、運用のための電子通貨発行運用組織に加盟してあるものとし、エンドユーザ5としての個人は、後述するように、携帯通信端末装置51を使用して自身で持つ口座預金の中か

ら必要金額だけ電子通貨に交換して引き落とし、その貨幣的価値情報をあらかじめ内蔵する記憶装置に設定してあるものとする。

ここで、電子通貨は、円やドルなどの基軸通貨に連動させてあるものとする。電子商取引には、商品の取引に加えて役務の取引も含まれる。商品には、銀行や証券会社が取扱う金融商品も含まれる。

#### 【 0 0 2 3 】

図 2 は、図 1 における携帯通信端末装置 5 1 の内部構成を示すブロック図であり、ここでは携帯電話端末が例示されている。図 2 に示すように、携帯電話端末は、基本的には、R F 回路 5 1 1、D S P (Digital Signal Processor) を核とするベースバンド L S I 5 1 2、マイクロプロセッサ 5 1 3、入出力インタフェース回路 5 1 4、L C D パネル 5 1 5、キーボードマウス 5 1 6、フラッシュメモリ 5 1 7、メモリカード 5 1 8、指紋認識カード 5 1 9 で構成される。

#### 【 0 0 2 4 】

ベースバンド L S I 5 1 2、マイクロプロセッサ 5 1 3、入出力インタフェース回路 5 1 4、フラッシュメモリ 5 1 7 は、内部バス 5 2 0 を介して共通に接続される。また、入出力インタフェース回路 5 1 4 には、更に、L C D パネル 5 1 5、キーボードマウス 5 1 6、メモリカード 5 1 8、指紋認識カード 5 1 9 が接続され、このメモリカード 5 1 8 ならびに指紋認識カード 5 1 9 は、携帯電話端末本体が持つカードスロットに着脱自在に実装されるものとする。ここでは、カードスロットとして P C カード規格に準拠したものを想定する。

#### 【 0 0 2 5 】

本発明実施形態では、指紋認識カード 5 1 9 として、富士通電装株式会社によって市販されている「Finger Pass Card」を使用するものとする。この指紋認識カード 5 1 9 は、P C カードスロットの標準である P C M C I A タイプ II に準拠するインタフェースを有し、スキャナとの一体化により、1 0 0 0 ～ 1 0 0 0 0 ユーザの指紋データを簡単に登録でき、照合のレベルに合わせて確実に照合が可能である。登録時にカードの末端（P C カードスロット接続部と対向する側）に位置するスキャナ部分に指を押圧し良好な指紋を登録しておけば照合時に良好な結果が得られる。ここでは、指紋の模様に含まれる特徴点の相対的なつながりを

利用して本人か他人かの識別精度を向上させる特徴相関法を用い特徴抽出を行っている。

尚、指紋認識カード 5 1 9 を用いることなく携帯通信端末装置 5 1 本体のみで指紋認識を行うことも可能である。この場合、LCD パネル 5 1 5 の少なくとも一部領域は、タブレットと一体型の構成となっており、後述するように、その領域に指を押圧することにより指紋データが採取され、本体内蔵の認識ドライバ（ソフトウェア）がこれを認識（特徴抽出）して外部にある認証サーバ 3 2 へ送信して照合操作を促す。

また、フラッシュメモリ 5 1 7 には、後述するプログラムや個人情報、場合によっては既に採取され、登録された指紋パターンが格納されており、メモリカード 5 1 8 には、プログラムによって処理されるデータが格納されるものとする。

#### 【 0 0 2 6 】

図 3 は、本発明実施形態の動作を説明するために引用したフローチャートであり、具体的には、携帯通信端末装置 5 1 が持つフラッシュメモリ、および流通系システム 2 にプログラムされ記録されるソフトウェアの処理手順を示すものであり、本発明と関係する部分のみ抽出してある。

#### 【 0 0 2 7 】

以下、図 3 に示すフローチャートを参照しながら、図 1、図 2 に示す本発明実施形態の動作について詳細に説明する。

まず、エンドユーザ 5 である個人は、自身の携帯通信端末装置 5 1（つまり携帯個人認証装置）を使って A T M オンラインシステムを利用し、あるいはインターネットに接続して銀行を含む各企業が提供するサービスシステムをアクセスする（ステップ S 3 1）。いずれも公衆回線網 6 を介してアクセスする。

ここでは、例えば、流通系の百貨店における商品メニューの表示を要求したとする。携帯通信端末装置 5 1 は、その要求に従う商品メニューを検索して流通系システム 2 から受信（ステップ S 3 2）した後、購入したい商品を選択し、その商品名と共に決済の仕方に関しキーボードマウス 5 1 6 を介して指示する（ステップ S 3 3）。

#### 【 0 0 2 8 】

このことにより、通信機器 51 内蔵のマイクロプロセッサ 513 は、フラッシュメモリ 517 にあらかじめ記録されてある個人情報領域をアクセスし、キャッシュ決済の場合は個人の識別番号（口座番号でも可）を、クレジット決済の場合はそのクレジット情報（ユーザ識別番号）をインターネット経由でサービスを提供している流通系企業へ送信する（ステップ S36、S45）。

## 【0029】

ここで、キャッシュ決済の場合、支払金額とメモリカード 518 に設定され、格納されてある価値残高情報との比較（ステップ S38）を行う。そして、その残高範囲内にあれば相当金額を引き出し（ステップ S42）商談は成立する。ない場合は、引き落とす旨利用者に確認し、ATM 機器 11 を介して銀行に接続して残高照会を行い、銀行預金口座に対する認証（ステップ S40）を行い、メモリカード 518 に対して所定金額の補充（ステップ S41）を行なう。そして先の引き出しで満たない金額相当を引き落とす（ステップ S42）。そして、初期の価値情報、残高、支払い実績等に関する情報を更新し、メモリカード 518 中に履歴として残す。

## 【0030】

ここで、銀行預金口座に対する認証は、利用者がパスワードを入力する手間を省くために、携帯通信端末装置 51 がフラッシュメモリ 517 の固定領域に書き込まれている個人情報領域をアクセスすることにより取引銀行に自動的に送信するものとする。または、利用者に対し、携帯通信端末装置 51 が持つ指紋認識カード 519 のセンサ領域に指を押圧することを促し、この結果、指紋認識カード 519 により、または指紋認識カード 519 を介して取込まれた指紋情報を受信して照合処理を行う。この照合処理は、銀行計算センタにある認証サーバ 32 で行われ、口座開設に際しあらかじめ採取された指紋情報との照合操作がなされ、自動的に認証が行われる。

尚、既に指紋が採取されフラッシュメモリ 517 の特定領域に格納されている場合は上記した手間を省くためにその登録済みの情報を自動的に送信する方法を採用しても良い。

## 【0031】

クレジット決済に関しても同様、フラッシュメモリ 5 1 7 の固定領域にカード識別番号等の個人情報が書き込まれており、この領域の内容をカード会社へ送信して認証の結果を得る。または、利用者に対し、携帯通信端末装置 5 1 が持つ指紋認識カード 5 1 9 のセンサ領域に指を押圧することを促し、この結果、採取された指紋情報を受信して照合処理を行う。照合処理は、銀行計算センタ 3 にある認証サーバ 3 2 に委ねるか、あるいは独自に用意するデータベースを用いて行われる。

#### 【 0 0 3 2 】

ここで、あらかじめ採取された指紋情報との照合操作がなされ、自動的に認証が行われる。カード会社は、カード識別番号あるいは指紋が適正か、また、希望商品を購入した場合、取引限度額を超えないか調べ、（ステップ S 4 6、S 4 7）その商品の受注処理へ進む。

尚、残高照会の結果、支払金額に見合う金額が預金口座にない場合は支払い不能とし、その旨、携帯電話 5 1 が持つ LCD パネル 5 1 5 に表示（ステップ S 4 3）して商談は不成立となる。また、クレジットに関しても残高不足の場合は支払い不能とし、その旨表示して商談は不成立となる。

#### 【 0 0 3 3 】

発注を受けた流通系企業では、その発注情報を受信することによって在庫を調べ、ある場合は決済処理を終了した旨と合わせて要求のあった通信機器 5 1 にインターネット経由で返答し、ない場合は、現在発注された商品在庫がない旨、更に入荷予定日をインターネット経由で携帯通信端末装置 5 1 に返答する。

#### 【 0 0 3 4 】

尚、携帯通信端末装置 5 1 が持つメモリカード 5 1 8 は、携帯通信端末装置 5 1 本体が持つ PC カードスロットに実装され、必要に応じて取り外し、たとえば、自動販売機システム 7 が持つカードスロットに装填することにより自販機支払いのための処理を行うことができる。また、ATM 機器 1 1 が持つカードスロットに実装することによっても電子通貨の交換をローカルに実行できる。

#### 【 0 0 3 5 】

図 4 は、本発明の携帯個人認証装置が携帯通信端末装置として使用される通報



システムの実施形態を示すブロック図である。図4は、自動車事故が発生したときに自動車41(42、4n)から自動的にSOS信号を発し、警察や消防、あるいは保険会社等所轄のセンタ45に緊急通報するシステムである。ここでは、全地球測位システム(GPS: Global Positioning System)の衛星電波を受信できるカーナビゲーションシステムを構成要素とする機器(通報システム搭載機器411)を各自動車41(~4n)に搭載し、緊急時に現在位置を知らせるSOS信号を携帯電話回線43経由で発信する仕組みを用いている。

具体的には、交通事故等でエアバッグが作動すると、搭載機器がGPSにより測位された現在位置や車体番号等の情報を自動的に発信する。これを24H体制のサービス会社44がキャッチし、自動車の位置やドライバの氏名、住所、自動車の番号を事故に最も近い警察局や消防署(所轄センタ45)に通報する。これは事故のみならず、ドライバが運転中に急病で発作を起こした場合にも手動で発信できるものとし、また、搭載機器は事故の衝撃にも耐えられるような航空機のフライトレコーダなみの強度を持つものとする。なお、GPSの衛星電波を受信できない場合は、カーナビゲーションシステムが備える光ファイバジャイロからのデータ、走行距離データなどと地図データを用いたマップマッチングにより、現在位置を知る。

#### 【0036】

上述した構成において、エアバッグ等が作動しても事故が軽微な場合もあり、また、機器の誤作動もある。この場合、運転者本人がこの通報システムを解除すれば問題は生じないが、大事故の場合、誰かが誤って、あるいは故意に解除することがありえる。このときに上述した個人認証機能を持つ携帯通信端末装置51(携帯個人認証装置)を使用して本人認証が行われ、サービス会社44を介して、あるいは所轄のセンタ45経由で解除の資格チェックが行われる。

認証のしくみについては図1に示す電子商取引システムと同様であり、重複を避ける意味でここでは述べないが、指紋は都度採取せず、あらかじめ内蔵するフラッシュメモリ517中に登録しておき、通報時、その情報を自動送信するしくみが必要となる場合もある。

#### 【0037】

尚、上述した実施形態では携帯通信端末装置 5 1 を兼ねる携帯個人認証装置として携帯電話端末を例示して説明したが、携帯電話端末に限らず、図 2 に示す基本構成を有する P D A 等各種モバイル機器で代用しても構わない。また、本発明実施形態では、本人認証のために指紋を用いたが、他に、声紋、虹彩紋、網膜紋、顔、署名等、生物学的特徴を有し、本人認証のために実績を有するものであれば代替することができる。

## 【 0 0 3 8 】

更に、指紋を採取、照合する手段として、市販の指紋認識カード 5 1 9 を携帯通信端末装置 5 1 が持つカードスロットに実装する例のみ示したが、これに制限されることなく、携帯通信端末装置本体にその機能を内蔵しても構わない。特に、最近の P D A の中には、表示入力一体型のものが多く、この場合、画像認識のための機能を本体に内蔵することが多い。従って P D A 本体に指紋認識のためのソフトウェアを持つことにより、P D A そのもので代用しても構わない。

また、電子通貨の記憶媒体としてメモリカード 5 1 8 のみ例示したが、これに制限されることなく、通信機器 5 1 本体に着脱自在に実装でき、リードライト可能なものであればその種類を問わない。

## 【 0 0 3 9 】

尚、本発明実施形態では、携帯個人認証装置を携帯通信端末装置として電子商取引システム、通報システムに適用した場合のみ説明したが、これに制限されず、自動車のリモコンによるキーレスエントリの代用として利用可能である。また、個人の認証だけに携帯個人認証装置を使用しても良い。例えば、警察等により不審尋問された場合の認証等種々利用可能である。また、警察や警備会社などが不信尋問を行う際の不審者の特定に使用しても良い。この場合、リファレンスとなる参照データを、携帯個人認証装置内に備えても良いし、前記実施形態のごとく認証サーバ内に備えても良い。また、通報システムとしての応用も多数考えられ、自動車事故はもとより、海山での遭難事故等にも威力を発する。

また、E T C における車載装置の作動許可や、定期券の券売機などの自動販売機をはじめ、個人認証を前提としたあらゆる電子システムに適用することができる。

【 0 0 4 0 】

【発明の効果】

以上説明のように本発明の携帯個人認証装置によれば、あらゆる用途に使用できる。本人認証のための手段として、指紋、声紋、虹彩紋、網膜紋、顔、署名等の生物学的特徴を用いることによってセキュリティ機能の充実がはかれる。

また、本発明の携帯個人認証装置に I C カード、クレジットカード等が持つ機能を内包させ、例えば A T M 機器と接続することにより、携帯個人認証装置を財布化して一元管理でき、また、各企業が構築するサービスシステムを取込むことによって各種商取引を簡単に実現できる。また、I C カードを電子通貨の媒体とする場合に比較して、パスワード入力等の煩わしさから解放される。更に、通信機器が持つ記憶装置内に使用履歴が都度格納され、必要に応じて残高等表示パネルにビジュアル表示されるため、履歴を含む現状把握が可能となり、利便性に富む。

【 0 0 4 1 】

更に、交通事故、遭難事故等発生の際、所轄センタへの緊急連絡解除時の本人認証のための手段としても本発明の携帯個人認証装置を用いることができる。この場合、全地球測位システム（G P S）の衛星電波を受信できる機器などを介して現在位置等を知らせる S O S 信号を任意の通信手段で所轄のセンタに通報するが、緊急連絡解除の際に携帯個人認証装置による通信手段で通信を行い、本人認証を受ける。これにより、機器の誤作動による、あるいは悪意の緊急連絡解除を防止することができ、このことにより、通報の確度が向上する。

【図面の簡単な説明】

【図 1】 本発明の一実施形態を示すブロック図である。

【図 2】 図 1 における携帯個人認証装置（携帯通信端末装置）の内部構成を示すブロック図である。

【図 3】 図 1 に示す本発明の一実施形態の概略動作を示すフローチャートである。

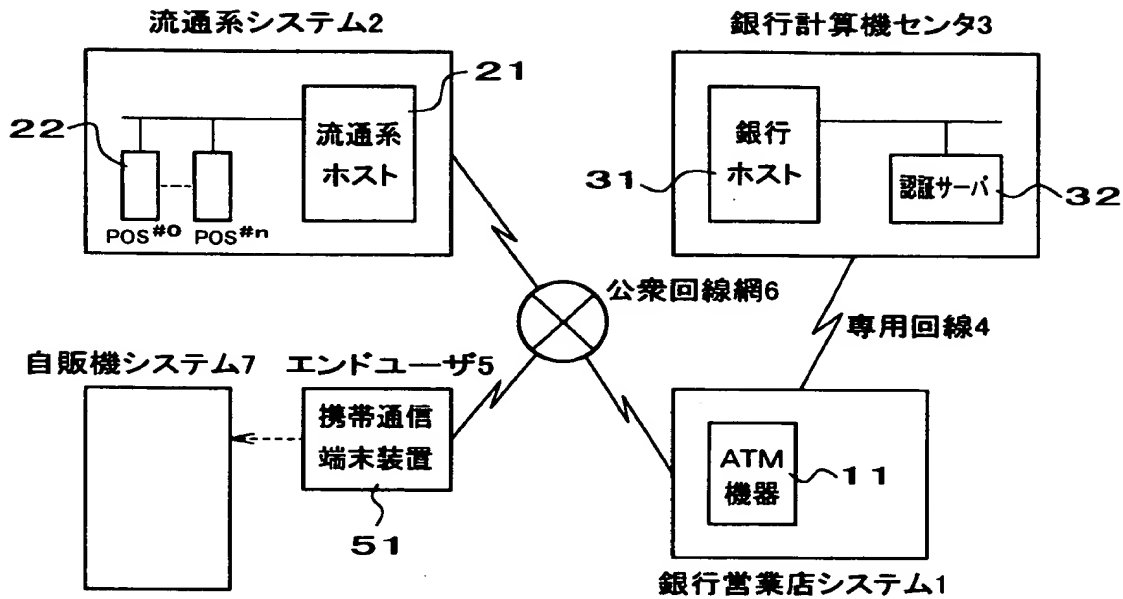
【図 4】 本発明の他の実施形態を示すブロック図である。

【符号の説明】

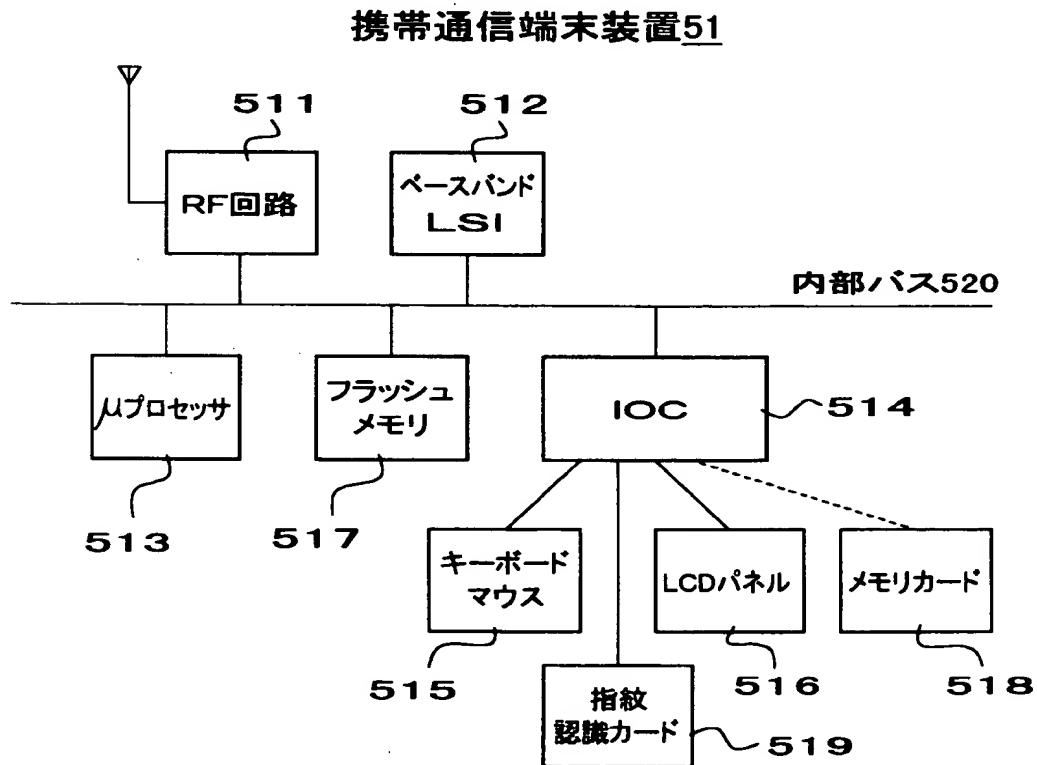
1…銀行営業店システム、2…流通系システム、3…銀行計算機センタ、4…専用回線、5…エンドユーザ、6…公衆回線網、7…自動販売機システム、11…ATM機器、21…流通系ホスト、31…銀行ホスト、32…認証サーバ、41(42、4n)…自動車、43…携帯電話回線網、44…サービス会社、45…所轄センタ、51…携帯通信端末装置(携帯個人認証装置)、511…RF回路、512…ベースバンドLSI、513…マイクロプロセッサ、514…入出力コントローラ、515…LCDパネル、516…キーボードマウス、517…フラッシュメモリ、518…メモリカード、519…指紋認証カード、520…内部バス

【書類名】 図面

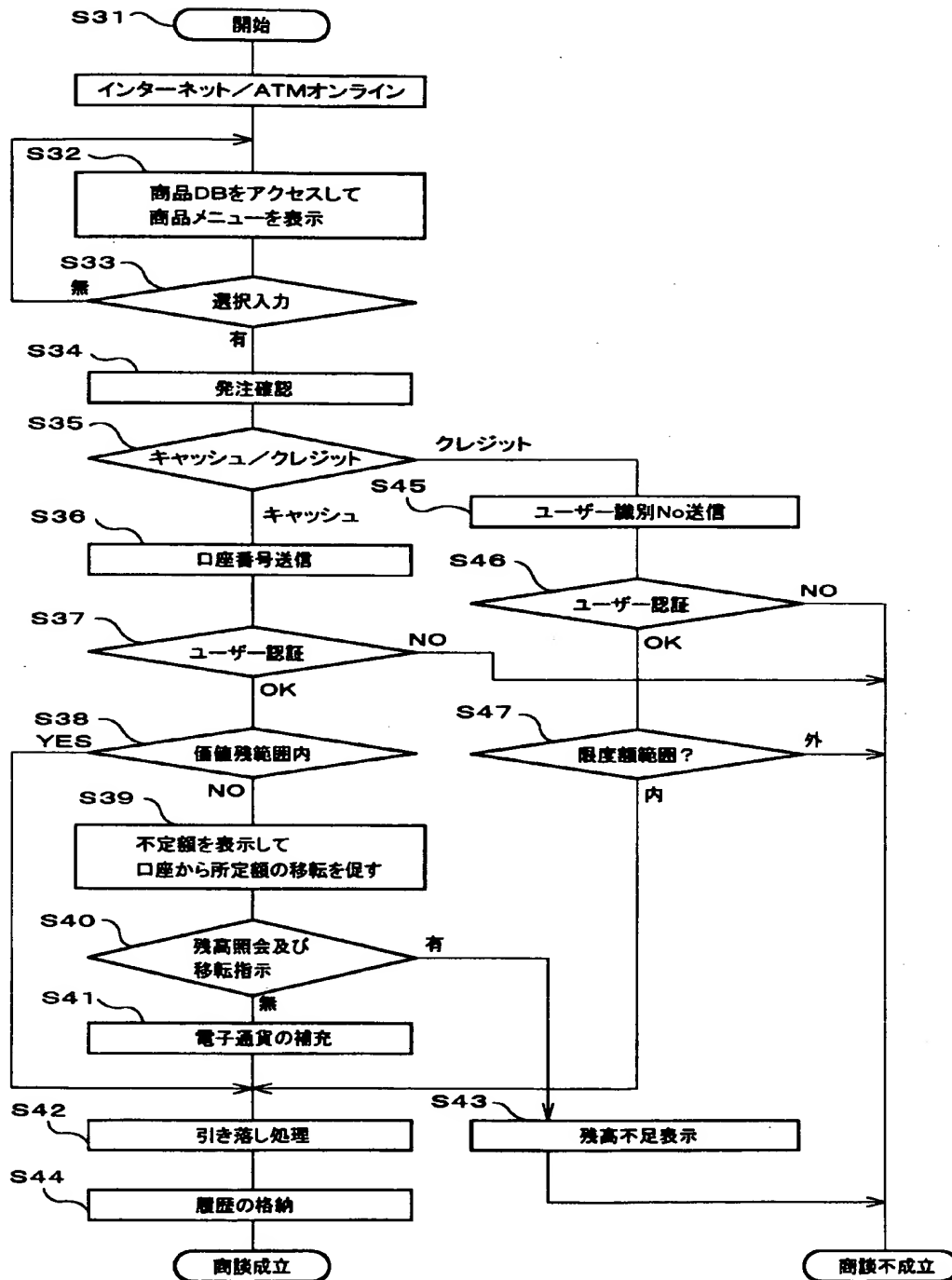
【図 1】



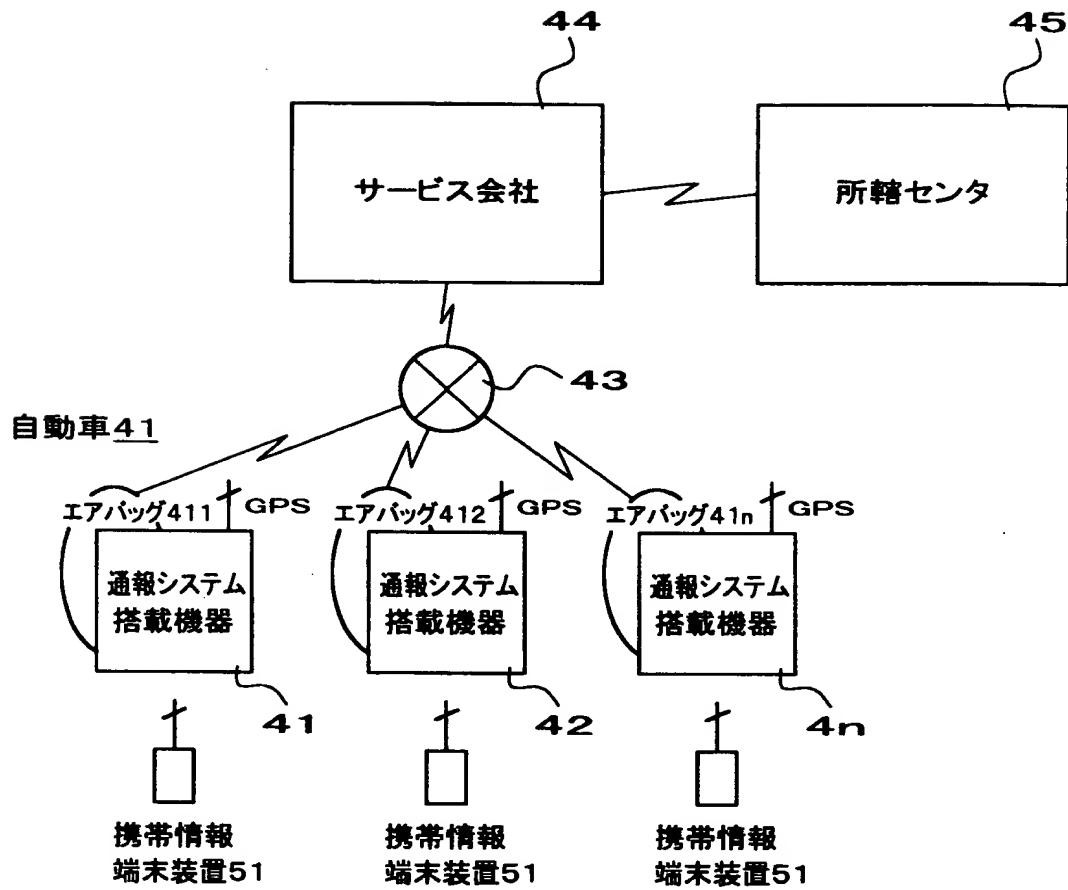
【図 2】



【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 今後の社会において必要不可欠となる個人の認証をどこでも行え、あらゆる用途に使用することのできる携帯個人認証装置及び同装置によりアクセスが許可される電子システムを提供することを目的とする。

【解決手段】 携帯個人認証装置を携帯通信端末装置 5 1 として、携帯電話や P D A 等のモバイル機器を使用し、生物学的特徴である、指紋、声紋、虹彩斑等のバイオメトリクス認証のうち少なくとも 1 つを本人認証のための手段として用いる。また、携帯通信端末装置（携帯個人認証装置）に従来 I C カード等が持っていた電子財布的な機能を内包させ、A T M 機器等と接続することによって電子財布としての一元管理を実現する。更に、携帯通信端末装置（携帯個人認証装置）を通報システムにおける緊急連絡解除のための本人認証に使用して通報の確度向上をはかる。

【選択図】 図 1



出 願 人 履 歴 情 報

識別番号 [000168207]

1. 変更年月日	1997年 6月11日
[変更理由]	住所変更
住 所	千葉県市川市菅野1-21-2
氏 名	溝部 達司

出 願 人 履 歴 情 報

識別番号 [596132905]

1. 変更年月日	1996年 9月10日
[変更理由]	新規登録
住 所	東京都小金井市中町2-22-28-211
氏 名	澤口 高司